Jennifer A. Hradil, Esq.
Justin T. Quinn, Esq.
GIBBONS P.C.
One Gateway Center
Newark, NJ 07102-5310
(973) 596-4500

Eugene F. Assaf, P.C., DC Bar 449778
Pro Hac Vice
K. Winn Allen, DC Bar 1000590
Pro Hac Vice
Jason M. Wilcox, DC Bar 1011415
Pro Hac Vice
KIRKLAND & ELLIS LLP
655 Fifteenth St. N.W.
Washington, D.C. 20005
(202) 879-5078

Douglas H. Meal, MA Bar 340971
Pro Hac Vice
David T. Cohen, MA Bar 670153
Pro Hac Vice
ROPES & GRAY LLP
Prudential Tower, 800 Boylston Street
Boston, MA 02199-3600
(617) 951-7517

Attorneys for Defendants

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF NEW JERSEY

FEDERAL TRADE COMMISSION Plaintiff, v. WYNDHAM WORLDWIDE CORPORATION, et al., Defendants.	CIVIL ACTION NO.: 2:13-CV-01887 (ES) (JAD) **DEFENDANTS' ANSWER TO PLAINTIFF'S FIRST AMENDED COMPLAINT**

DEFENDANTS' ANSWER TO PLAINTIFF'S

FIRST AMENDED COMPLAINT

Defendants Wyndham Worldwide Corp., Wyndham Hotels and Resorts, LLC, Wyndham Hotel Group, LLC, and Wyndham Hotel Management, Inc. (collectively, "Defendants") answer Plaintiff's First Amended Complaint as follows:

1. The FTC brings this action under Section 13(b) of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 53(b), to obtain permanent injunctive relief and other equitable relief for Defendants' acts or practices in violation of Section 5(a) of the FTC Act, 15 U.S.C. § 45(a), in connection with Defendants' failure to maintain reasonable and appropriate data security for consumers' sensitive personal information.

ANSWER: To the extent the allegations in paragraph 1 are legal conclusions, no response is required. To the extent any response is required, Defendants deny that they failed to maintain reasonable and appropriate data security for consumers' sensitive personal information or violated the statutes cited in the Commission's allegations. Defendants also deny that Plaintiff is entitled to any relief under those statutes.

2. Defendants' failure to maintain reasonable security allowed intruders to obtain unauthorized access to the computer networks of Wyndham Hotels and Resorts, LLC, and several hotels franchised and managed by Defendants on three separate occasions in less than two years. Defendants' security failures led to fraudulent charges on consumers' accounts, more than $10.6 million in fraud loss, and the export of hundreds of thousands of consumers' payment card account information to a domain registered in Russia. In all three security breaches, hackers accessed sensitive consumer data by compromising Defendants' Phoenix, Arizona data center.

ANSWER: Defendants lack knowledge sufficient to form a belief as to whether hackers accessed sensitive consumer data by compromising Defendants' Phoenix, Arizona data center. Defendants deny the remaining allegations in paragraph 2, except to acknowledge that unidentified, sophisticated cybercriminals gained unauthorized access to Hotels and Resorts' computer network and the separate computer networks maintained by certain Wyndham-branded hotels.

JURISDICTION AND VENUE

3. This Court has subject matter jurisdiction pursuant to 28 U.S.C. §§ 1331, 1337(a), and 1345, and 15 U.S.C. §§ 45(a) and 53(b).

ANSWER: To the extent the allegations in paragraph 3 are legal conclusions, no response is required. To the extent any response is required, Defendants admit that Plaintiff purports to assert claims under 15 U.S.C. § 45(a), but deny that Defendants violated the statutes cited by Plaintiff and that Plaintiff is entitled to any relief under those statutes.

4. Venue is proper in this district under 28 U.S.C. § 1391(b), (c), and 15 U.S.C. § 53(b).

ANSWER: To the extent the allegations in paragraph 4 are legal conclusions, no response is required. To the extent any response is required, Defendants admit that Plaintiff purports to assert claims under the FTC Act, but deny that Defendants violated that statute and that Plaintiff is entitled to any relief under that statute. Defendants admit that venue is proper in the District of New Jersey.

PLAINTIFF

5. The FTC is an independent agency of the United States Government created by statute. 15 U.S.C. §§ 41-58. The FTC enforces Section 5(a) of the FTC Act, 15 U.S.C. § 45(a), which prohibits unfair or deceptive acts or practices in or affecting commerce.

ANSWER: To the extent the allegations in paragraph 5 are legal conclusions, no response is required. To the extent any response is required, Defendants admit that Plaintiff purports to assert claims under the FTC Act, but deny that Defendants violated the statutes cited by Plaintiff and that Plaintiff is entitled to any relief under those statutes. Defendants lack knowledge sufficient to admit or deny allegations about the legal status of the FTC.

6. The FTC is authorized to initiate federal district court proceedings, by its own attorneys, to enjoin violations of the FTC Act and to secure such equitable relief as may be appropriate in each case. 15 U.S.C. § 53(b).

ANSWER: To the extent the allegations in paragraph 6 are legal conclusions, no response is required. To the extent any response is required, Defendants admit that Plaintiff purports to assert claims under the FTC Act, but deny that they violated the statutes cited by Plaintiff or that Plaintiff is entitled to any relief under those statutes. Defendants lack knowledge sufficient to admit or deny allegations about the legal status of the FTC.

DEFENDANTS

7. Defendant Wyndham Worldwide Corporation ("Wyndham Worldwide") is a Delaware corporation with its principal office or place of business at 22 Sylvan Way, Parsippany, New Jersey 07054. At all times material to this Complaint, Wyndham Worldwide has been in the hospitality business, franchising and managing hotels throughout the United States. Wyndham Worldwide transacts or has transacted business in this district and throughout the United States. At all relevant times, it has controlled the acts and practices of its subsidiaries described below and approved of or benefitted from such subsidiaries' acts and practices at issue in this Complaint. See Exhibit A for an organizational chart depicting the entities named as Defendants in this Complaint.

ANSWER: Defendants admit that Wyndham Worldwide is a Delaware corporation with its principal office or place of business at 22 Sylvan Way, Parsippany, New Jersey 07054. Defendants also admit that Wyndham Worldwide has been in the hospitality business, including franchising and managing hotels through subsidiaries, and that it indirectly transacts business throughout the United States through subsidiaries. Defendants deny all other allegations in paragraph 7. To the extent the allegations in paragraph 7 purport to characterize written documents, the terms of which speak for themselves, no response is required.

8. Defendant Wyndham Hotel Group, LLC ("Hotel Group") is a Delaware limited liability company with its principal office or place of business at 22 Sylvan Way, Parsippany,

New Jersey 07054. Hotel Group operates a datacenter in Phoenix, Arizona (the "Phoenix data center") that it uses to store and process payment card data, and the payment card data of some of its subsidiaries, including Wyndham Hotels and Resorts, LLC. Hotel Group is a wholly-owned subsidiary of Wyndham Worldwide, and through its subsidiaries it franchises and manages approximately 7,000 hotels under twelve hotel brands, one of which is the Wyndham brand. It transacts or has transacted business in this district and throughout the United States. At all relevant times, Hotel Group has controlled the acts and practices of its subsidiaries described below and approved of or benefitted from such subsidiaries' acts and practices at issue in this Complaint.

ANSWER: Defendants admit that Hotel Group is a Delaware limited liability company with its principal office or place of business at 22 Sylvan Way, Parsippany, New Jersey 07054. Defendants admit that Hotel Group operates a datacenter in Phoenix, Arizona. Defendants admit that Hotel Group is a wholly-owned subsidiary of Wyndham Worldwide and that through its subsidiaries it franchises and manages approximately 7,000 hotels under twelve operating hotel brands, one of which is the Wyndham brand. Defendants admit that Hotel Group transacts or has transacted business in this district and throughout the United States. Defendants deny all other allegations in paragraph 8.

9. Defendant Wyndham Hotels and Resorts, LLC ("Hotels and Resorts") is a Delaware limited liability company with its principal office or place of business at 22 Sylvan Way, Parsippany, New Jersey 07054. Hotels and Resorts is a wholly-owned subsidiary of Hotel Group. Throughout the relevant time period, Hotels and Resorts has licensed the Wyndham name to independent hotels through franchise agreements, and provided various services to those hotels, including information technology services. At all times material to this Complaint, Hotels and Resorts has licensed the Wyndham name to approximately seventy-five independently-owned hotels under franchise agreements. Hotels and Resorts transacts or has transacted business in this district and throughout the United States, including franchising hotels located in Arizona. At all relevant times, Hotel Group and Wyndham Worldwide have performed various business functions on behalf of Hotels and Resorts, or overseen such business functions, including legal assistance, human resources, finance, and information technology and security. Hotel Group and Wyndham Worldwide controlled the acts and practices of Hotels and Resorts that are at issue in this Complaint.

ANSWER: Defendants admit that Hotels and Resorts is a Delaware limited liability company with its principal office or place of business at 22 Sylvan Way, Parsippany, New Jersey 07054 and that it is a wholly-owned subsidiary of Hotel Group. Defendants admit

that throughout the relevant time period, Hotels and Resorts has licensed the Wyndham name to independent hotels through franchise agreements, and provides various services to those hotels. Defendants admit that Hotels and Resorts has transacted business in this district and throughout the United States. Defendants admit that Hotel Group and Wyndham Worldwide have performed various business functions on behalf of Hotels and Resorts, or overseen such business functions, including legal assistance, human resources, finance, and information technology and security. Defendants deny all other allegations in paragraph 9.

10. Defendant Wyndham Hotel Management, Inc. ("Hotel Management") is a Delaware corporation with its principal office or place of business at 22 Sylvan Way, Parsippany, New Jersey 07054. Hotel Management is also a wholly-owned subsidiary of Hotel Group. Like Hotels and Resorts, Hotel Management licenses the Wyndham name to independently-owned hotels, but does so under management agreements in which it agrees to fully operate the hotel on behalf of the owner. At all times material to this Complaint, Hotel Management has licensed the Wyndham name to approximately fifteen independently-owned hotels under management agreements. Hotel Management transacts or has transacted business in this district and throughout the United States, including managing at least one hotel in Arizona. At all relevant times, Hotel Group and Wyndham Worldwide have performed various business functions on Hotel Management's behalf, or overseen such business functions, including legal assistance and information technology and security. Hotel Group and Wyndham Worldwide controlled the acts and practices of Hotel Management that are at issue in this Complaint.

ANSWER: Defendants admit that Hotel Management is a Delaware Corporation with its principal office or place of business at 22 Sylvan Way, Parsippany, New Jersey 07054 and that it is a wholly-owned subsidiary of Hotel Group. Defendants admit that Hotel Management operates independently-owned hotels in the Wyndham name on behalf of the owners. Defendants admit that Hotel Management transacts business in this district and in limited parts of the United States. Defendants admit that Hotel Group and Wyndham Worldwide have performed various business functions on behalf of Hotel Management, or overseen such business functions, including legal assistance, human

resources, finance, and information technology and security. Defendants deny all other allegations in paragraph 10.

11. Defendants Wyndham Worldwide, Hotel Group, Hotels and Resorts, and Hotel Management have operated as a common business enterprise while engaging in the unfair and deceptive acts and practices alleged in this Complaint. Defendants have conducted their business practices described below through an interrelated network of companies that have common ownership, business functions, employees, and office locations. Because these Defendants have operated as a common enterprise, they are jointly and severally liable for the unfair and deceptive acts and practices alleged below.

ANSWER: Defendants deny the allegations in paragraph 11.

COMMERCE

12. At all times material to this Complaint, Defendants have maintained a substantial course of trade in or affecting commerce, as "commerce" is defined in Section 4 of the FTC Act, 15 U.S.C. § 44.

ANSWER: Defendants admit the allegations in paragraph 12.

DEFENDANTS' BUSINESS ACTIVITIES

Defendants' Business Structure

13. Wyndham Worldwide is a hospitality business that, through its subsidiaries, franchises and manages hotels and sells timeshares. It conducts its business through three subsidiaries, including Hotel Group. At all times relevant to this Complaint, Hotel Group's wholly-owned subsidiaries, Hotels and Resorts and Hotel Management, licensed the Wyndham brand name to approximately ninety independently-owned hotels under franchise or management agreements (collectively hereinafter "Wyndham-branded hotels").

ANSWER: Defendants admit that Wyndham Worldwide and its subsidiaries are engaged in the hospitality business and that Hotels and Resorts franchises and Hotel Management manages hotels. Defendants admit that Wyndham Worldwide conducts its business through three divisions, including Hotel Group. Defendants admit that, at all times relevant to this Complaint, Hotels and Resorts licensed the Wyndham brand name to independently-owned hotels under franchise agreements and that Hotel Management

operated independently-owned hotels in the Wyndham name on behalf of the owners. Defendants deny all other allegations in paragraph 13.

Defendants' Network Infrastructure

14. Throughout the relevant time period, Wyndham Worldwide has been responsible for creating information security policies for itself and its subsidiaries, including Hotel Group and Hotels and Resorts, as well as providing oversight of their information security programs. From at least 2008 until approximately June 2009, Hotel Group had responsibility for managing Hotels and Resorts' information security program. In June 2009, Wyndham Worldwide took over management and responsibility for Hotels and Resorts' information security program.

ANSWER: Defendants admit that from at least 2008 until approximately June 2009, Hotel Group had responsibility for managing Hotels and Resorts' information security program. Defendants also admit that in June 2009, Wyndham Worldwide took over management and responsibility for Hotels and Resorts' information security program. Defendants deny the remaining allegations in paragraph 14, except to acknowledge that Wyndham Worldwide had created information security polices for itself.

15. Under their franchise and management agreements, Hotels and Resorts and Hotel Management require each Wyndham-branded hotel to purchase, and configure to their specifications, a designated computer system, known as a property management system, that handles reservations, checks guests in and out, assigns rooms, manages room inventory, and handles payment card transactions. These property management systems store personal information about consumers, including names, addresses, email addresses, telephone numbers, payment card account numbers, expiration dates, and security codes (hereinafter "personal information").

ANSWER: Defendants lack knowledge sufficient to admit or deny allegations about what information each property's Property Management Systems store. Defendants deny the remaining allegations in paragraph 15, except to acknowledge that Wyndham-branded hotels are required to purchase a property management system and that property management systems (among other things) handle reservations, check guests in and out, assign rooms, manage room inventory, and handle payment card transactions.

16. The property management systems for all Wyndham-branded hotels, including those managed by Hotel Management, are part of Hotels and Resorts' computer network, and are linked to its corporate network, much of which is located in the Phoenix data center. Hotels and Resorts' corporate network includes its central reservation system, which coordinates reservations across the Wyndham brand.

ANSWER: Defendants deny the allegations in paragraph 16, except to acknowledge that Hotels and Resorts' central reservation system is part of Hotels and Resorts' network.

17. Each Wyndham-branded hotel's property management system is managed by Defendants. Only Defendants, and not the owners of the Wyndham-branded hotels, have administrator access that allows Defendants to control the property management systems at the hotels. Defendants set the rules, including all password requirements, that allow the Wyndham-branded hotels' employees to access their property management systems.

ANSWER: Defendants deny the allegations in paragraph 17.

18. Defendants have even more direct control over the computer networks of the Wyndham-branded hotels managed by Hotel Management. Hotel Management controls the "operation" of those hotels pursuant to its management agreements, including their information technology and security functions and the hiring of employees to administer the hotels' computer networks.

ANSWER: Defendants deny the allegations in paragraph 18, except to acknowledge that Hotel Management in some cases has some control over the hiring of certain employees and that Wyndham Worldwide and Hotel Group in some cases have some control over the technology and security functions of the managed hotels.

19. The owners of the Wyndham-branded hotels pay Defendants fees to support their property management systems and to connect them to Hotels and Resorts' computer network. Defendants' technical support team is responsible for addressing and resolving any technical issues that a Wyndham-branded hotel has with its property management system. As explained further below, Defendants' information security failures led to the compromise of many of the Wyndham-branded-hotels' property management system servers, resulting in the exposure of thousands of consumers' payment card accounts.

ANSWER: Defendants deny the allegations in paragraph 19, except to admit that owners of the Wyndham-branded hotels pay Defendants fees for certain services (including technology support).

DEFENDANTS' DECEPTIVE STATEMENTS

20. Hotels and Resorts operates a website where consumers can make reservations at any Wyndham-branded hotel. In addition, some Wyndham-branded hotels operate their own individual websites, which describe the individual hotel and its amenities. Customers making reservations from a Wyndham-branded hotel's individual website are directed back to Hotels and Resorts' website to make the reservation.

ANSWER: Defendants admit that Hotels and Resorts operates a website where consumers can make reservations at certain Wyndham-branded hotels and that some Wyndham-branded hotels operate their own individual websites. Defendants lack knowledge sufficient to admit or deny what the content is of each Wyndham-branded hotel's website or whether all such websites direct users back to Hotels and Resorts' website to make reservations, and therefore deny the remaining allegations in paragraph 20.

21. Since at least 2008, Defendants have disseminated, or caused to be disseminated, privacy policies or statements on their website to their customers and potential customers. These policies or statements include, but are not limited to, the following statement regarding the privacy and confidentiality of personal information, disseminated on the Hotels and Resorts' website:

> ... We recognize the importance of protecting the privacy of individual-specific (personally identifiable) information collected about guests, callers to our central reservation centers, visitors to our Web sites, and members participating in our Loyalty Programs (collectively 'Customers')....
>
> This policy applies to residents of the United States, hotels of our Brands located in the United States, and Loyalty Program activities in the United States only....
>
> We safeguard our Customers' personally identifiable information by using industry standard practices. Although "guaranteed security" does not exist either on or off the Internet, we make commercially reasonable efforts to make our collection of such Information consistent with all applicable laws and regulations. Currently, our Web sites utilize a variety of different security measures designed to protect personally identifiable information from unauthorized access by users both inside and outside of our company, including the use of 128-bit encryption based on a Class 3 Digital Certificate issued by Verisign Inc. This allows for utilization of Secure Sockets Layer, which is a method for encrypting data. This protects confidential information - such as credit card numbers, online forms, and

> financial data - from loss, misuse, interception and hacking. We take commercially reasonable efforts to create and maintain "fire walls" and other appropriate safeguards to ensure that to the extent we control the Information, the Information is used only as authorized by us and consistent with this Policy, and that the Information is not improperly altered or destroyed.

ANSWER: To the extent the allegations in paragraph 21 purport to characterize written documents, the terms of which speak for themselves, no further response is required. Defendants admit that since 2008, Hotels and Resorts, Hotel Group, and Wyndham Worldwide have included privacy policies on their websites. Defendants deny all other allegations in paragraph 21.

22. There is a link to this privacy policy on each page of the Hotels and Resorts' website, including its reservations page.

ANSWER: Defendants deny the allegations in paragraph 22, except to acknowledge that there is currently a link to a different privacy policy on Hotels and Resorts' website.

23. Although this statement is disseminated on the Hotels and Resorts' website, it states that it is the privacy policy of Hotel Group.

ANSWER: To the extent the allegations in paragraph 23 purport to characterize written documents, the terms of which speak for themselves, no response is required. Defendants deny all other allegations in paragraph 23.

DEFENDANTS' INADEQUATE DATA SECURITY PRACTICES

24. Since at least April 2008, Defendants failed to provide reasonable and appropriate security for the personal information collected and maintained by Hotels and Resorts, Hotel Management, and the Wyndham-branded hotels, by engaging in a number of practices that, taken together, unreasonably and unnecessarily exposed consumers' personal data to unauthorized access and theft. Among other things, Defendants:

a. failed to use readily available security measures to limit access between and among the Wyndham-branded hotels' property management systems, the Hotels and Resorts' corporate network, and the Internet, such as by employing firewalls;

b. allowed software at the Wyndham-branded hotels to be configured inappropriately, resulting in the storage of payment card information in clear readable text;

c. failed to ensure the Wyndham-branded hotels implemented adequate information security policies and procedures prior to connecting their local computer networks to Hotels and Resorts' computer network;

d. failed to remedy known security vulnerabilities on Wyndham-branded hotels' servers that were connected to Hotels and Resorts' computer network, thereby putting personal information held by Defendants and the other Wyndham-branded hotels at risk. For example, Defendants permitted Wyndham-branded hotels to connect insecure servers to the Hotels and Resorts' network, including servers using outdated operating systems that could not receive security updates or patches to address known security vulnerabilities;

e. allowed servers to connect to Hotels and Resorts' network, despite the fact that well-known default user IDs and passwords were enabled on the servers, which were easily available to hackers through simple Internet searches;

f. failed to employ commonly-used methods to require user IDs and passwords that are difficult for hackers to guess. Defendants did not require the use of complex passwords for access to the Wyndham-branded hotels' property management systems and allowed the use of easily guessed passwords. For example, to allow remote access to a hotel's property management system, which was developed by software developer Micros Systems, Inc., Defendants used the phrase "micros" as both the user ID and the password;

g. failed to adequately inventory computers connected to the Hotels and Resorts' network so that Defendants could appropriately manage the devices on its network;

h. failed to employ reasonable measures to detect and prevent unauthorized access to Defendants' computer network or to conduct security investigations;

i. failed to follow proper incident response procedures, including failing to monitor Hotels and Resorts' computer network for malware used in a previous intrusion; and

j. failed to adequately restrict third-party vendors' access to Hotels and Resorts' network and the Wyndham-branded hotels' property management systems, such as by restricting connections to specified IP addresses or granting temporary, limited access, as necessary.

ANSWER: Defendants deny the allegations in paragraph 24.

INTRUSIONS INTO DEFENDANTS' COMPUTER NETWORK

25. As a result of the failures described above, between April 2008 and January 2010, intruders were able to gain unauthorized access to Hotels and Resorts' computer network, including the Wyndham-branded hotels' property management systems, on three separate occasions. The intruders used similar techniques on each occasion to access personal information stored on the Wyndham-branded hotels' property management system servers, including customers' payment card account numbers, expiration dates, and security codes. After discovering each of the first two breaches, Defendants failed to take appropriate steps in a reasonable time frame to prevent the further compromise of the Hotels and Resorts' network.

ANSWER: Defendants deny the allegations in paragraph 25, except to admit that, during some period of time from April 2008 to January 2010, unidentified, sophisticated cybercriminals gained unauthorized access to Hotels and Resorts' computer network and the separate computer networks of certain Wyndham-branded hotels.

First Breach

26. In April 2008, intruders first gained access to a Phoenix, Arizona Wyndham-branded hotel's local computer network that was connected to the Internet. The hotel's local network was also connected to Hotels and Resorts' network through the hotel's property management system. Using this access, in May 2008, the intruders attempted to compromise an administrator account on the Hotels and Resorts' network by guessing multiple user IDs and passwords—known as a brute force attack.

ANSWER: Defendants lack knowledge sufficient to admit or deny the allegations in paragraph 26, except to admit that, in or about April 2008, unidentified, sophisticated cybercriminals gained unauthorized access to the separate computer network of a Wyndham-branded hotel. Defendants therefore deny the remaining allegations in paragraph 26.

27. This brute force attack caused multiple user account lockouts over several days, including one instance in which 212 user accounts were locked out, before the intruders were ultimately successful. Account lockouts occur when a user inputs an incorrect password multiple times, and are a well-known warning sign that a computer network is being attacked. Defendants did not have an adequate inventory of the Wyndham-branded hotels' computers connected to its network, and, therefore, although they were able to determine that the account lockouts were coming from two computers on Hotels and Resorts' network, they were unable to

physically locate those computers. As a result, Defendants did not determine that the Hotels and Resorts' network had been compromised until almost four months later.

ANSWER: Defendants admit that account lockouts can occur when a user inputs an incorrect password multiple times and that account lockouts can occur as a result of unauthorized login attempts. Defendants lack knowledge sufficient to admit or deny whether a brute force attack caused user account lockouts. Defendants therefore deny those and all of the remaining allegations in paragraph 27.

28. The intruders' brute force attack led to the compromise of an administrator account on the Hotels and Resorts network. Because Defendants did not appropriately limit access between and among the Wyndham-branded hotels' property management systems, the Hotels and Resorts' own corporate network, and the Internet—such as through the use of firewalls—once the intruders had access to the administrator account, they were able to gain unfettered access to the property management system servers of a number of hotels.

ANSWER: Defendants lack knowledge sufficient to admit or deny whether the intruders' brute force attack led to the compromise of an administrator account on the Hotels and Resorts network. Defendants deny the remaining allegations in paragraph 28, except to acknowledge that unidentified, sophisticated cybercriminals gained unauthorized access to Hotels and Resorts' computer network and the separate computer networks of certain Wyndham-branded hotels.

29. Additionally, the Phoenix hotel's property management system server was using an operating system that its vendor had stopped supporting, including providing security updates and patch distribution, more than three years prior to the intrusion. Defendants were aware the hotel was using this unsupported and insecure server, yet continued to allow it to connect to Hotels and Resorts' computer network.

ANSWER: Defendants deny the allegations in paragraph 29, except to acknowledge that Hotels and Resorts instructed the Phoenix property to upgrade its property management system prior to the first intrusion.

30. In this first breach, the intruders installed memory-scraping malware on numerous Wyndham-branded hotels' property management system servers, thereby accessing payment

card data associated with the authorization of payment card transactions that was present temporarily on the hotels' servers.

ANSWER: Defendants lack knowledge sufficient to admit or deny the allegations in paragraph 30, except to acknowledge that the cybercriminals introduced memory-scraping malware into individual servers of certain of the Wyndham-branded hotels in an effort to access payment card data associated with authorization of payment card transactions that was present transitorily in the servers' random access memory. Defendants therefore deny the remaining allegations in paragraph 30.

31. In addition, the intruders located files on some of the Wyndham-branded hotels' property management system servers that contained payment card account information for large numbers of consumers, stored in clear readable text. These files were created and stored in clear text because Defendants had allowed the property management systems to be configured inappropriately to create these files and store the payment card information that way.

ANSWER: Defendants admit that cybercriminals were able to locate files on some of the Wyndham-branded hotels' servers that contained payment card account information stored in clear readable text, due to the failure of a third party to properly configure the systems that they created and provided to the Wyndham-branded hotels. Defendants deny the remaining allegations in paragraph 31.

32. As a result of Defendants' unreasonable data security practices, intruders were able to gain unauthorized access to the Hotels and Resorts' corporate network, and the property management system servers of forty-one Wyndham-branded hotels—twelve managed by Hotel Management and twenty-nine franchisees of Hotels and Resorts. This resulted in the compromise of more than 500,000 payment card accounts, and the export of hundreds of thousands of consumers' payment card account numbers to a domain registered in Russia.

ANSWER: Defendants deny the allegations in paragraph 32, except to acknowledge that unidentified, sophisticated cybercriminals gained unauthorized access to Hotels and Resorts' computer network and the separate computer networks of certain Wyndham-branded hotels.

Second Breach

33. In March 2009, approximately six months after Defendants discovered the first breach, intruders were able again to gain unauthorized access to the Hotels and Resorts' network, this time through a service provider's administrator account in the Phoenix data center.

ANSWER: Defendants lack knowledge sufficient to admit or deny the allegations in paragraph 33, except to acknowledge that in or about March 2009 unidentified, sophisticated cybercriminals gained unauthorized access to Hotels and Resorts' computer network.

34. In May 2009, Defendants learned that several Wyndham-branded hotels had received complaints from consumers about fraudulent charges made to their payment card accounts after using those cards to pay for stays at Wyndham-branded hotels. At that point, Defendants searched Hotels and Resorts' network for the memory-scraping malware used in the previous attack, and found it on the property management system servers of more than thirty Wyndham-branded hotels. As a result of Defendants' failure to monitor Hotels and Resorts' network for the malware used in the previous attack, hackers had unauthorized access to the Hotels and Resorts' network for approximately two months.

ANSWER: Defendants deny the allegations in paragraph 34, except to acknowledge that in May 2009 Defendants discovered that in or about March 2009 unidentified, sophisticated cybercriminals gained unauthorized access to Hotels and Resorts' computer network and the networks of certain Wyndham-branded hotels and Defendants took action to contain and expel the malware and remediate the intrusion.

35. In addition to again using memory-scraping malware to access personal information, in this second breach the intruders reconfigured software at the Wyndham-branded hotels to cause their property management systems to create clear text files containing the payment card account numbers of guests using their payment cards at the hotels.

ANSWER: Defendants lack knowledge or information sufficient to form a belief as to the truth of the allegations in paragraph 35 and therefore deny them.

36. Ultimately, the intruders exploited Defendants' data security vulnerabilities to gain access to the Hotels and Resorts' network and the property management system servers of thirty-nine Wyndham-branded hotels—nine of which were managed by Hotel Management and thirty franchisees of Hotels and Resorts. In this second incident, the intruders were able to

access information for more than 50,000 consumer payment card accounts and use that information to make fraudulent charges on consumers' accounts.

ANSWER: Defendants deny the allegations in paragraph 36, except to acknowledge that unidentified, sophisticated cybercriminals gained unauthorized access to Hotels and Resorts' computer network and the separate computer networks of certain Wyndham-branded hotels.

Third Breach

37. In late 2009, intruders again compromised an administrator account on Hotels and Resorts' network. Because Defendants had still not adequately limited access between and among the Wyndham-branded hotels' property management systems, Hotels and Resorts' corporate network, and the Internet such as through the use of firewalls—once the intruders had access to this administrator account they were able again to access multiple Wyndham-branded hotels' property management system servers. As in the previous attacks, the intruders installed memory-scraping malware to access payment card account information held at the Wyndham-branded hotels.

ANSWER: Defendants lack knowledge sufficient to admit or deny the allegations in the first and third sentences of paragraph 37, except to acknowledge that in or about late 2009, unidentified, sophisticated cybercriminals gained unauthorized access to Hotels and Resorts' computer network and the separate computer networks of certain Wyndham-branded hotels and installed memory-scraping malware on the servers of certain Wyndham-branded hotels. Defendants deny the remaining allegations in paragraph 37.

38. Again, Defendants did not detect this intrusion themselves, but rather learned of the breach from a credit card issuer. The credit card issuer contacted Defendants in January 2010, and indicated that the account numbers of credit cards it had issued were used fraudulently shortly after its customers used their credit cards to pay for stays at Wyndham-branded hotels.

ANSWER: Defendants admit that a credit card issuer contacted Defendants in January 2010 and indicated that the account numbers of credit cards it had issued were used fraudulently. Defendants deny the remainder of paragraph 38.

39. As a result of Defendants' security failures, in this instance, intruders compromised Hotels and Resorts' corporate network and the property management system servers of twenty-eight Wyndham-branded hotels—eight managed by Hotel Management and twenty franchisees of Hotels and Resorts. As a result of this third incident, the intruders were able to access information for approximately 69,000 consumer payment card accounts and again make fraudulent purchases on those accounts.

ANSWER: Defendants deny the allegations in paragraph 39, except to acknowledge that unidentified, sophisticated cybercriminals gained unauthorized access to Hotels and Resorts' computer network and the separate computer networks of certain Wyndham-branded hotels.

Total Impact of Breaches

40. Defendants' failure to implement reasonable and appropriate security measures exposed consumers' personal information to unauthorized access, collection, and use. Such exposure of consumers' personal information has caused and is likely to cause substantial consumer injury, including financial injury, to consumers and businesses. For example, Defendants' failure to implement reasonable and appropriate security measures resulted in the three data breaches described above, the compromise of more than 619,000 consumer payment card account numbers, the exportation of many of those account numbers to a domain registered in Russia, fraudulent charges on many consumers' accounts, and more than $10.6 million in fraud loss. Consumers and businesses suffered financial injury, including, but not limited to, unreimbursed fraudulent charges, increased costs, and lost access to funds or credit. Consumers and businesses also expended time and money resolving fraudulent charges and mitigating subsequent harm.

ANSWER: Defendants deny the allegations in paragraph 40.

VIOLATIONS OF THE FTC ACT

41. Section 5(a) of the FTC Act, 15 U.S.C. § 45(a), prohibits "unfair or deceptive acts or practices in or affecting commerce."

ANSWER: To the extent the allegations in paragraph 41 are legal conclusions, no response is required. To the extent any response is required, Defendants deny that they violated the statute cited by Plaintiff and that Plaintiff is entitled to any relief under that statute.

42. Misrepresentations or deceptive omissions of material fact constitute deceptive acts or practices prohibited by Section 5(a) of the FTC Act.

ANSWER: To the extent the allegations in paragraph 42 are legal conclusions, no response is required. To the extent any response is required, Defendants deny that they violated the statute cited by Plaintiff and that Plaintiff is entitled to any relief under that statute.

43. Acts or practices are unfair under Section 5 of the FTC Act if they cause or are likely to cause substantial injury to consumers that consumers cannot reasonably avoid themselves and that is not outweighed by countervailing benefits to consumers or competition. 15 U.S.C. § 45(n).

ANSWER: To the extent the allegations in paragraph 43 are legal conclusions, no response is required. To the extent any response is required, Defendants deny that they violated the statute cited by Plaintiff and that Plaintiff is entitled to any relief under that statute.

Count I
Deception

44. In numerous instances through the means described in Paragraph 21, in connection with the advertising, marketing, promotion, offering for sale, or sale of hotel services, Defendants have represented, directly or indirectly, expressly or by implication, that they had implemented reasonable and appropriate measures to protect personal information against unauthorized access.

ANSWER: Defendants deny the allegations in paragraph 44.

45. In truth and in fact, in numerous instances in which Defendants have made the representations set forth in Paragraph 44 of this Complaint, Defendants did not implement reasonable and appropriate measures to protect personal information against unauthorized access.

ANSWER: Defendants deny the allegations in paragraph 45.

46. Therefore, Defendants' representations as set forth in Paragraph 44 of this Complaint are false or misleading and constitute deceptive acts or practices in violation of Section 5(a) of the FTC Act, 15 U.S.C. § 45(a).

ANSWER: Defendants deny the allegations in paragraph 46.

Count II
Unfairness

47. In numerous instances Defendants have failed to employ reasonable and appropriate measures to protect personal information against unauthorized access.

ANSWER: Defendants deny the allegations in paragraph 47.

48. Defendants' actions caused or are likely to cause substantial injury to consumers that consumers cannot reasonably avoid themselves and that is not outweighed by countervailing benefits to consumers or competition.

ANSWER: Defendants deny the allegations in paragraph 48.

49. Therefore, Defendants' acts and practices as described in Paragraph 47 above constitute unfair acts or practices in violation of Section 5 of the FTC Act, 15 U.S.C. §§ 45(a) and 45(n).

ANSWER: Defendants deny the allegations in paragraph 49.

CONSUMER INJURY

50. Consumers have suffered and will continue to suffer substantial injury as a result of Defendants' violations of the FTC Act. In addition, Defendants have been unjustly enriched as a result of their unlawful acts or practices. Absent injunctive relief by this Court, Defendants are likely to continue to injure consumers, reap unjust enrichment, and harm the public interest.

ANSWER: Defendants deny the allegations in paragraph 50.

THIS COURT'S POWER TO GRANT RELIEF

51. Section 13(b) of the FTC Act, 15 U.S.C. § 53(b), empowers this Court to grant injunctive and such other relief as the Court may deem appropriate to halt and redress violations of any provision of law enforced by the FTC. The Court, in the exercise of its equitable jurisdiction, may award ancillary relief, including rescission or reformation of contracts, restitution, the refund of monies paid, and the disgorgement of ill-gotten monies, to prevent and remedy any violation of any provision of law enforced by the FTC.

ANSWER: To the extent the allegations in paragraph 51 are legal conclusions, no response is required. To the extent any response is required, Defendants deny that they

violated the statutes cited by Plaintiff and that Plaintiff is entitled to any relief under those statutes.

PRAYER FOR RELIEF

Wherefore, Plaintiff FTC, pursuant to Section 13(b) of the FTC Act, 15 U.S.C. § 53(b), and the Court's own equitable powers, requests that the Court:

A. Enter a permanent injunction to prevent future violations of the FTC Act by Defendants;

B. Award such relief as the Court finds necessary to redress injury to consumers resulting from Defendants' violations of the FTC Act, including but not limited to, rescission or reformation of contracts, restitution, the refund of monies paid, and the disgorgement of ill-gotten monies; and

C. Award Plaintiff the costs of bringing this action, as well as such other and additional relief as the Court may determine to be just and proper.

ANSWER: Defendants deny that any relief is appropriate.

DEFENSES

In addition to the foregoing responses, Defendants generally deny liability for all claims alleged in the Amended Complaint and deny each allegation that has not been specifically admitted. Defendants assert the following specific defenses in response to Plaintiff's claims, undertaking the burden of proof only as to those defenses deemed affirmative defenses by law, regardless of how such defenses are designated herein. Defendants reserve all rights to assert additional defenses as they become known in the course of discovery.

FIRST DEFENSE: Plaintiff lacks statutory authority to assert the claims alleged in the Complaint.

SECOND DEFENSE: Plaintiff has failed to provide constitutionally adequate fair notice of the requirements for data security pursuant to Section 5 of the FTC Act.

THIRD DEFENSE: Plaintiff cannot prove "substantial injury to consumers" as required by Section 5 of the FTC Act. *See* 15 U.S.C. § 45(n).

FOURTH DEFENSE: **Any consumer injury was "reasonably avoidable by consumers themselves," barring Plaintiff's FTC Act claims. *See* 15 U.S.C. § 45(n).**

FIFTH DEFENSE: **Plaintiff cannot prove that any act or practice "is likely to cause" substantial injury to consumers as required by Section 5 of the FTC Act. *See* 15 U.S.C. § 45(n).**

SIXTH DEFENSE: **Plaintiff cannot prove that any act or practice violated an established public policy.**

SEVENTH DEFENSE: **The statements that are the basis for Count 1 are inaccurate.**

EIGHTH DEFENSE: **Plaintiff cannot prove that any misrepresentations were material.**

NINTH DEFENSE: **No Defendant can be held derivatively liable, under a theory of common enterprise or otherwise, for any Section 5 violation committed by another Defendant.**

TENTH DEFENSE: **Plaintiff cannot prove causation as required by Section 5 of the FTC Act.**

ELEVENTH DEFENSE: **Defendants cannot be held liable for a Section 5 violation committed by their franchisees or licensees.**

TWELFTH DEFENSE: **Defendants cannot be held liable for a Section 5 violation committed by a service provider.**

THIRTEENTH DEFENSE: **Plaintiff is not entitled to any relief because this is not a "proper case" for relief within the meaning of Section 13(b) of the FTC Act insofar as any**

violation of Section 5 that may have occurred was not clear and in any event is not likely to recur.

FOURTEENTH DEFENSE: Plaintiff cannot prove that any injunctive relief it might request is appropriate.

FIFTEENTH DEFENSE: Plaintiff cannot prove that equitable monetary relief is appropriate.

WHEREFORE, Defendants deny that Plaintiff is entitled to any relief whatsoever and respectfully request judgment dismissing Plaintiff's complaint with prejudice, and any such further relief as may be allowed by law.

RESERVATION OF RIGHTS

Defendants reserve the right to amend this Answer or to assert other defenses as this action proceeds. Based on all the foregoing as well as other grounds, Defendants deny that they violated any of the statutes cited by Plaintiff and that the Plaintiff is entitled to any relief whatsoever.

Dated: July 17, 2014

Respectfully submitted,

/s/ Jennifer A. Hradil

By: _____

Jennifer A. Hradil, Esq.
Justin T. Quinn, Esq.
GIBBONS P.C.
One Gateway Center
Newark, NJ 07102-5310
(973) 596-4500

Eugene F. Assaf, P.C., DC Bar 449778
Pro Hac Vice
K. Winn Allen, DC Bar 1000590
Pro Hac Vice
Jason M. Wilcox, DC Bar 1011415

Pro Hac Vice
KIRKLAND & ELLIS LLP
655 Fifteenth St. N.W.
Washington, D.C. 20005
(202) 879-5078

Douglas H. Meal, MA Bar 340971
Pro Hac Vice
David T. Cohen, MA Bar 670153
Pro Hac Vice
ROPES & GRAY LLP
Prudential Tower, 800 Boylston Street
Boston, MA 02199-3600
(617) 951-7517

Attorneys for Defendants

CERTIFICATE OF SERVICE

The undersigned certifies that on this 17th day of July, 2014, all counsel of record who are deemed to have consented to electronic service are being served with a copy of this document through the Court's CM/ECF system.

By: */s/ Jennifer A. Hradil*